宝信网络巡警 eCop 在政府的应用

一、项目背景

该政府网络由政府中心、各委办局和各街道共同组成，包括涉密网、内部网（业务网）、外部网（公开网站等）三个部分。随着政务网网络基础服务平台的逐渐形成，政府大院内接入单位有 40 余家；院外接入单位达到近 100 家。其中内部业务网应用直接支撑外网应用，承载大财政、大审计，同时连接工商、教育、公安等纵向网络，构成完整一体化的电子政务应用平台。总的节点数千台，院内网段 40 多个。此次内网管理主要针对内部业务网。

该政府内网管理的特点：

1、涉密等级：网络中有涉密网，与政府公务网相连，涉及到政府信息的安全。不能与其它网络连接。

2、涉密单位结构：该政府业务网接入了众多机关单位，每个单位都担负着政府职能运行的职责，所以每个单位都很重要，院内和院外的单位加起来有 140 多个。该政府是分级管理的，以政府大院为中心，包含各街道和各委办局共同组成。

3、信息化程度：政府信息化程度比较高，信息化到一定程度，势必会引发内网安全的需求，需要加强内部网络管理的需求。

4、信息中心人员素质：

（1）政府信息安全中心肩负着网络（设备），网络安全，服务器，主机运行维护的任务，在单位是比较重要的部门。

（2）政府信息安全中心领导相对是弱势地位，客户端的实施可能需要中心的人员自己去安装。

该政府内网资源的特点：

1、终端分散程度：政府二级机构和接入单位比较多，所以网段数目也多；内网节点总数比较多，信息点院内位置分布集中，院外分布分散。

2、软件自动分发：没有自动分发工具，没有域管理策略。

3、终端计算机性能：政府计算机大多性能良好。

4、常用软件：政府使用操作系统：Windows98，Windows2000 系列，WindowsXP，

Windows2003Server；有私自接桌面路由器的情况，对 IP 地址管理阻断会有影响。

二、 问题与需求分析

政府内网信息安全的基本需求如下：

1、内外网隔离

政府目前计算机都装了隔离卡。

2、外联监控

政府的涉密网内的计算机不让访问外部计算机或者 Internet；业务网的计算机不能访问 Internet。

3、资产管理

目前政府的资产管理还没有通过技术手段，还是通过手工在管理，所以对资产信息管理的需求迫切。

4、节点接入控制

对于不是该内网的计算机接入内网，希望能对该未登记注册的计算机进行快速隔离和阻断。对于内部非法修改终端计算机网络设置的计算机能进行验证，即节点验证的需求。

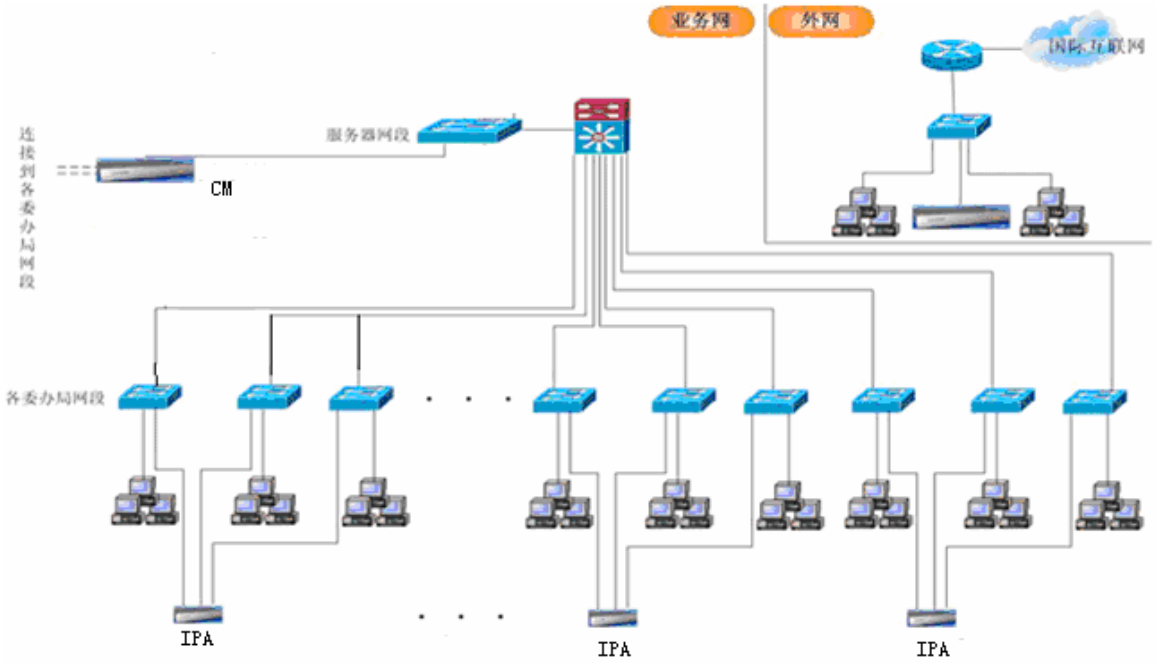
对于大楼中裸露物理网口的保护。

5、服务器监控

内网中的计算机是很多都是通过服务器来获取网络共享资源，如果服务器宕掉，或者其中运行关键服务关键进程出现问题，将影响到内网信息的可获得性，也是影响信息安全的一个重大问题。

三、方案设计

eCop 中心控制器部署政府网中心机房的服务器网段内。客户端管理程序安装在各个被管理二级部门的终端计算机上。整个实施方案工作的示意图如下：



政府内网 eCop 部署示意图

具体实现功能如下：

节点接入控制与 IP 违规变更

该功能专注于网络接入安全，解决了内网中计算机设备非法接入、IP 地址违规变更的问题，提高网络的可用性和可靠性。

eCop 的该项功能可以实时扫描与分析在线计算机的 IP、MAC 地址信息，管理员可验证各项信息，通过 IP-MAC 绑定、DHCP-MAC 绑定和特权 MAC 配置三种方式将接入设备设定为合法，而对于非法机器则进行警告并实现隔离阻断。

这里的“非法机器”含两种情况：一是外来接入的新机器，未经过管理员验证绑定过的；二是经过管理员验证的原合法机器，因更改了 IP 或 DHCP 地址使原合法绑定失效的。如此，不仅控制了新节点的非法接入，也对内部 IP 地址的违规变更、冒用、盗用提供有力的解决方案。

资产管理

该功能可按组织结构管理，实现设备信息的注册和审批，自动收集终端的系统、硬件、软件信息；信息变更时，自动记录，并可根据策略向管理员发送报警，信息可搜索查询，可导出 excel 报表。如此不仅可以对网段内各终端计算机的软硬件信息了如指掌，出现违规事件可以定位到人，还可以根据需要对信息进行选择查询，形成的统计数据，为单位硬件升级、信息上报等提供方便。

管理人员可在中央控制器设定启用或禁用各终端计算机的外设和端口，包括软驱、光驱、U 盘、MODEM、串口、并口、红外接口、1394 口等外围设备和接口，即使断开内网，客户端程序照样具有控制作用。该功能的最大特点就是启用与关闭的方便与灵活，且对 U 盘的禁用不会影响到 USB 键盘、鼠标的应用。

管理人员还可在中央控制器设定内网计算机要求运行和禁止运行的进程列表，客户端程序对终端计算机进行监控，发现的违规进程进行报警，发现禁止进程可自动停止其运行。

非法外联监控

该功能可定周期检测终端计算机的网络连接情况，记录下其违规外联的信息并向中央控制器发送违规记录和报警，对于发生非法外联行为的计算机，客户端可自动断开其各种网络连接，包括网卡连接、拨号连接、无线连接等。

客户端程序运行于终端计算机的后台，即使断开内网而外联，客户端程序也可检测到。另外，非法外联监控策略可灵活配置，无须外网监控服务器。

服务监控

该功能可实现 Web、数据库等政府重要服务的性能状态监控，一旦发现状态异常可向管理员进行报警。

四、 方案实施与效果

整个方案的实施大致分为三个阶段：

1、 试用的阶段。信息中心的人员先在自己部门小范围内试用，测试没有问题后大规模部署。

2、 大规模部署安装客户端阶段。因为没有任何客户端分发软件，所以 ecop 客户端安装占据了相当大的工作量。

3、 IP 地址管理启用，全网阻断上线阶段。信息中心在全部网段开启阻断，将未安装客户端的主机和未经许可上线的主机隔离于局域网之外。

在部署过程中，和用户的交流非常重要，而且需要很耐心，对政府机关单位来说这点很重要。

部署 eCop 之前，由于网络分布广，结构复杂，管理人员人手不足等原因，该政府网络存在管理困难的情况，例如内部使用设备管理不是很严格，导致非法外联现象的泛滥；虽然内部网络的 IP 地址、资产管理有成制度化，但信息中心由于责权有限，无法有效的对整个网络

的维护起到监督和有效管理。

eCop 的使用为区政府信息网络运行管理带来了非常好的保障：

首先，区政府内、专网要求与公网完全物理隔离，宝信网络巡警的非法外联管理模块对网络的非法外联现象进行管理，禁止了非法上网等情况，大大减低了信息泄露和病毒感染的可能性；

其次，eCop 的计算机资产信息管理模块解决了私自购买、接驳计算机外部设备的问题，它的禁用功能可以控制计算机软驱、光驱、U 盘和调制解调器的使用，还有自动收集资产信息的功能（硬件信息、软件信息）给设备资产的登记带来了很大方便；

第三，eCop 的 IP 地址管理模块解决了 IP 地址管理的有章无序的问题，对于擅自修改 IP 地址或非法连入网络的现象给与了有效的控制，因为它可以阻断来自外部擅自接入专网的计算机和擅自更改 IP 地址的计算机。